

JUL 17 2008

SCHWEGMAN ■ LUNDBERG ■ WOESSNER

Patent Protection for High Technology

P.O. Box 2938

Minneapolis, MN 55402

Telephone (612) 373-6900

Facsimile (612) 339-3061

Date: 7/17/08Time: 4:20
(Minneapolis, Minn.)TO: Commissioner for Patents
Attn: Andrew Kim
Patent Examining Corps
P.O. Box 1450
Alexandria, VA 22313-1450
FAX NUMBER 571-273-8300FROM: Rodney L. LacyOUR REF: 1842.046US1TELEPHONE: 571-272-1691**571-273-1691**

Document(s) Transmitted: Applicant-Initiated Interview Request Form and Proposed Amendments for interview only, not for submission (2 pages); Amendments for interview purposes only not for submission (9 pages).

Total pages of this transmission, including cover letter: 11Please e-mail confirmation of receipt to akramber@slwip.com immediately upon receipt.In re: Patent Application of: Thomas A. Gentles et al.Examiner: Andrew KimSerial No.: 10/824,945Group Art Unit: 3713Filed: April 15, 2004Docket No.: 1842.046US1Title: REMOTE AUTHENTICATION OF GAMING SOFTWARE IN A GAMING SYSTEM ENVIRONMENTPlease see the attached proposed amendments for use during the in-person interview on ~~date~~ July 22, 2008. Thank you,By: [Signature]
Name: Rodney L. Lacy
Reg. No.: 41,136

RECEIVED
CENTRAL FAX CENTER

JUL 17 2008

Modified Form PTOL-413A (10-07)
Based on form approved for use through 5/31/2008

Applicant Initiated Interview Request Form

Application No.: 10/824,945 First Named Applicant: Thomas A. Gentles
Examiner: Andrew Kim Art Unit: 3714 Status of Application: Pending

Tentative Participants:

(1) Rodney L. Lacy (2) Michael Blankstein
(3) Andrew Kim (4) John Hotaling

Proposed Date of Interview: July 22, 2008 Proposed Time: To be determined

Type of Interview Requested:

(1) ☐ Telephonic (2) ☒ Personal (3) ☐ Video Conference

Please contact attorney Rodney L. Lacy at (612) 373-6954 with any questions concerning the comments or amendments proposed in this request.

Exhibit To Be Shown or Demonstrated: ☐ YES ☐ NO
If yes, provide brief description:

Issues To Be Discussed

Issues (Rej., Obj., etc)	Claims/ Fig. #s	Cited Art	Discussed	Agreed	Not Agreed
(1) 35 USC 102	1-3, 5-8, 10-11, 13-15, 17-22	US 7,043,641 (Martinek)	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(2) 35 USC 103	4, 9, 12, 16	Martinek	<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(3)			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>
(4)			<input type="checkbox"/>	<input type="checkbox"/>	<input type="checkbox"/>

☐ Continuation sheet attached.

Brief Description of Arguments to be Presented:

Discussion of how proposed amendments distinguish over Martinek.

An interview was conducted on the above-identified application on _____.

NOTE: This form should be completed by applicant and submitted to the examiner in advance of the interview (see MPEP § 713.01)

This application will not be delayed from issue because of applicant's failure to submit a written record of this interview. Therefore, applicant is advised to file a statement of the substance of this interview (37 CFR 1.133(b)) as soon as possible.

Applicant/Applicant's Representative Signature

Examiner/SPE Signature

Rodney L. Lacy

Typed/Printed Name of Applicant or Representative

41,136

Registration Number, if applicable

SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450.

RECEIVED
CENTRAL FAX CENTER

JUL 17 2008

AMENDMENT AND RESPONSE UNDER 37 CFR § 1.111

Page 1
Dkt: 1842.046US1

Serial Number: 10/824,945

Filing Date: April 15, 2004

Title: REMOTE AUTHENTICATION OF GAMING SOFTWARE IN A GAMING SYSTEM ENVIRONMENT

S/N 10/824,945PATENTIN THE UNITED STATES PATENT AND TRADEMARK OFFICE

Applicant: Thomas A. Gentles et al.

Examiner: Andrew Kim

Serial No.: 10/824,945

Group Art Unit: 3713

Filed: April 15, 2004

Docket No.: 1842.046US1

Title: REMOTE AUTHENTICATION OF GAMING SOFTWARE IN A GAMING
SYSTEM ENVIRONMENTPROPOSED AMENDMENT
NOT FOR ENTRY - FOR DISCUSSION ONLY

1. (Currently Amended) A method, performed by a gaming system server, comprising:
performing an authentication routine of an executable gaming software program, by
exchanging messages with a gaming terminal over a communication network, wherein the
authentication routine results in a determination of whether a copy of the executable gaming
software program stored at a gaming terminal is substantially identical to a copy of the
executable gaming software program accessible by the gaming system server; and
upon determining the copy of the executable gaming software program stored at the
gaming terminal is not substantially identical to the copy of the executable gaming software
program accessible by the gaming system server, gathering forensic data associated with the
operation of the executable software program.
2. (Original) The method of claim 1, wherein performing the authentication routine
comprises:
forming a first message digest, which includes an encrypted version of a first software
program component combined with a seed value;
transmitting the seed value over a communication network to a gaming terminal;
receiving, from the gaming terminal, a second message digest, which includes an
encrypted version of a second software program component and the seed value;
comparing the second message digest to the first message digest; and
authenticating the second software program component if the first message digest is
substantially identical to the second message digest.

AMENDMENT AND RESPONSE UNDER 37 CFR § 1.111

Serial Number: 10/824,945

Filing Date: April 15, 2004

Title: REMOTE AUTHENTICATION OF GAMING SOFTWARE IN A GAMING SYSTEM ENVIRONMENT

Page 2

Dkt: 1842.046US1

3. (Original) The method of claim 2, wherein forming the first message digest comprises:
generating the seed value by a random number generator;
appending the seed value to the first software program component to form a combined first software program, the first software program component assumed to be substantially equivalent to the second software program component; and
applying a cryptographic method to the combined first software program to form the first message digest.
4. (Original) The method of claim 2, wherein transmitting the seed value comprises transmitting the seed value over a virtual private network.
5. (Currently Amended) A method, performed by a gaming terminal, comprising:
receiving one or more authentication-related messages from a gaming system server over a communication network; [[and]]
sending at least one responsive message to the gaming system server, in response to receiving the one or more authentication-related messages, in order to enable the gaming system server to authenticate a copy of an executable gaming software program stored at the gaming terminal; and
upon determining the copy of the executable gaming software program stored at the gaming terminal is not authentic, gathering forensic data associated with the operation of the executable software program.
6. (Original) The method of claim 5, wherein receiving the one or more authentication-related messages comprises:
receiving a seed value over the communication network from the gaming system server.
7. (Original) The method of claim 6, further comprising:
forming a first message digest, which includes an encrypted version of the seed value combined with a first software program component within the gaming terminal; and

AMENDMENT AND RESPONSE UNDER 37 CFR § 1.111

Serial Number: 10/824,945

Filing Date: April 15, 2004

Title: REMOTE AUTHENTICATION OF GAMING SOFTWARE IN A GAMING SYSTEM ENVIRONMENT

Page 3

Dkt: 1842.046US1

wherein sending the at least one responsive message includes transmitting the first message digest over the communication network to the gaming system server.

8. (Original) The method of claim 7, wherein forming the first message digest comprises:
appending the seed value to the first software program component to form a combined first software program; and
applying a cryptographic method to the combined first software program to form the first message digest.
9. (Original) The method of claim 7, wherein transmitting the first message digest comprises transmitting the first message digest over a virtual private network.
10. (Currently Amended) A method comprising:
a gaming system server forming a first message digest, which includes an encrypted version of a first software program component combined with a seed value;
transmitting the seed value over a communication network to a gaming terminal;
receiving, from the gaming terminal, a second message digest, which includes an encrypted version of a second software program component and the seed value;
comparing the second message digest to the first message digest; [[and]]
authenticating the second software program component if the first message digest is substantially identical to the second message digest; and
upon determining the copy of the executable gaming software program stored at the gaming terminal is not authentic, gathering forensic data associated with the operation of the executable software program.
11. (Original) The method of claim 10, wherein forming the first message digest comprises:
generating the seed value by a random number generator;

AMENDMENT AND RESPONSE UNDER 37 CFR § 1.111

Serial Number: 10/824,945

Filing Date: April 15, 2004

Title: REMOTE AUTHENTICATION OF GAMING SOFTWARE IN A GAMING SYSTEM ENVIRONMENT

Page 4

Dkt: 1842.046US1

appending the seed value to the first software program component to form a combined first software program, the first software program component assumed to be substantially equivalent to the second software program component; and

applying a cryptographic method to the combined first software program to form the first message digest.

12. (Original) The method of claim 10, wherein transmitting the seed value comprises transmitting the seed value over a virtual private network.

13. (Original) The method of claim 10, wherein the gaming system server initiates taking the gaming terminal out of service when the first message digest is not substantially identical to the second message digest.

14. (Original) A method comprising:

receiving, by a gaming terminal, a seed value over a communication network from a gaming system server;

forming a first message digest, which includes an encrypted version of the seed value combined with a first software program component within the gaming terminal; and

transmitting the first message digest over the communication network to the gaming system server.

15. (Original) The method of claim 14, wherein forming the first message digest comprises:

appending the seed value to the first software program component to form a combined first software program; and

applying a cryptographic method to the combined first software program to form the first message digest.

16. (Original) The method of claim 14, wherein transmitting the first message digest comprises transmitting the first message digest over a virtual private network.

AMENDMENT AND RESPONSE UNDER 37 CFR § 1.111

Serial Number: 10/824,945

Filing Date: April 15, 2004

Title: REMOTE AUTHENTICATION OF GAMING SOFTWARE IN A GAMING SYSTEM ENVIRONMENT

Page 5

Dkt: 1842.046US1

17. (Currently Amended) In a gaming system having a plurality of gaming devices interconnected by a communication network, a method comprising:

a first gaming device remotely authenticating a first software program component within a second gaming device that is remotely located from the first gaming device, wherein remote authentication is performed by selecting a seed value generated by a random number generator;

appending the seed value to a second software program component to form a combined second software program, the second software program component substantially equivalent to the first software program component;

applying a cryptographic method to the combined second software program to form a first message digest;

transmitting the seed value to the second gaming device having the first software program component;

receiving a second message digest from the second gaming device, the second message digest formed by applying the cryptographic method to a combined first software program component, the combined first software program component formed by appending the seed value to the first software program component;

comparing the second message digest to the first message digest; [[and]]

authenticating the first software program component if the first message digest is substantially identical to the second message digest; and

upon determining the copy of the executable gaming software program stored at the gaming terminal is not authentic, gathering forensic data associated with the operation of the executable software program.

18. (Original) The method of claim 17, wherein the first gaming device includes a server in a jurisdictional data center, and wherein the second gaming device includes a gaming terminal in a casino customer network.

AMENDMENT AND RESPONSE UNDER 37 CFR § 1.111

Serial Number: 10/824,945

Filing Date: April 15, 2004

Title: REMOTE AUTHENTICATION OF GAMING SOFTWARE IN A GAMING SYSTEM ENVIRONMENT

Page 6
Dkt: 1842.046US1

19. (Original) The method of claim 17, wherein the first gaming device includes a server in a casino customer corporate center, and wherein the second gaming device includes a gaming terminal in a casino customer network associated with the casino customer corporate center.

20. (Currently Amended) A gaming system comprising:

a gaming system server, which performs an authentication routine of an executable gaming software program, by exchanging messages with a gaming terminal over a communication network, wherein the authentication routine results in a determination of whether a copy of the executable gaming software program stored at a gaming terminal is substantially identical to a copy of the executable gaming software program accessible by the gaming system server; [[and]]

one or more gaming terminals, interconnected with the at least one gaming system server over the communication network; and

a data storage unit operable to store forensic data;

wherein the authentication routine obtains the forensic data from the data storage unit in response to a determination that the copy of the executable gaming software program is not authentic.

21. (Original) A computer-readable medium having program instructions stored thereon to perform a method, which when executed within an electronic device, result in:

a gaming system server performing an authentication routine of an executable gaming software program, by exchanging messages with a gaming terminal over a communication network, wherein the authentication routine results in a determination of whether a copy of the executable gaming software program stored at a gaming terminal is substantially identical to a copy of the executable gaming software program accessible by the gaming system server.

22. (Original) A computer-readable medium having program instructions stored thereon to perform a method, which when executed within an electronic device, result in:

a gaming terminal receiving one or more authentication-related messages from a gaming system server over a communication network; and

AMENDMENT AND RESPONSE UNDER 37 CFR § 1.111

Page 7

Serial Number: 10/824,945

Dkt: 1842.046US1

Filing Date: April 15, 2004

Title: REMOTE AUTHENTICATION OF GAMING SOFTWARE IN A GAMING SYSTEM ENVIRONMENT

sending at least one responsive message to the gaming system server, in response to receiving the one or more authentication-related messages, in order to enable the gaming system server to authenticate a copy of an executable gaming software program stored at the gaming terminal.

RECEIVED
CENTRAL FAX CENTER

JUL 17 2008

Page 8

Dkt: 1842.046US1

AMENDMENT AND RESPONSE UNDER 37 CFR § 1.111

Serial Number: 10/824,945

Filing Date: April 15, 2004

Title: REMOTE AUTHENTICATION OF GAMING SOFTWARE IN A GAMING SYSTEM ENVIRONMENT

REMARKS

This responds to the Office Action mailed on February 26, 2008.

Claims ____ are amended, claims ____ are canceled, and claims ____ are added; as a result, claims ____ are now pending in this application.

Interview Summary

Applicant thanks Examiner Andrew Kim for the courtesy of a telephone interview on N/A with Applicant's representative Steven W. Lundberg.

[ATTORNEY, summarize interview with examiner.]

§102 Rejection of the Claims

Claims 1-3, 5-8, 10-11, 13-15 and 17-22 were rejected under 35 U.S.C. § 102(e) for anticipation by Martinek et al. (U.S. Patent 7,043,641).

§103 Rejection of the Claims

Claims 4, 9, 12 and 16 were rejected under 35 U.S.C. § 103(a) as being unpatentable over Martinek et al. (U.S. Patent 7,043,641).

RECEIVED
CENTRAL FAX CENTER

JUL 17 2008

AMENDMENT AND RESPONSE UNDER 37 CFR § 1.111

Serial Number: 10/824,945

Filing Date: April 15, 2004

Title: REMOTE AUTHENTICATION OF GAMING SOFTWARE IN A GAMING SYSTEM ENVIRONMENT

Page 9

Dkt: 1842.046US1

CONCLUSION

Applicants respectfully submit that the claims are in condition for allowance, and notification to that effect is earnestly requested. The Examiner is invited to telephone Applicants' attorney at (612) 373-6902 to facilitate prosecution of this application.

If necessary, please charge any additional fees or credit overpayment to Deposit Account No. 19-0743.

Respectfully submitted,

SCHWEGMAN, LUNDBERG & WOESSNER, P.A.
P.O. Box 2938
Minneapolis, MN 55402
(612) 373-6902

Date _____

By _____
Steven W. Lundberg
Reg. No. 30,568

CERTIFICATE UNDER 37 CFR 1.8: The undersigned hereby certifies that this correspondence is being filed using the USPTO's electronic filing system EFS-Web, and is addressed to: Mail Stop Amendment, Commissioner of Patents, P.O. Box 1450, Alexandria, VA 22313-1450 on this ____ day of July 2008.

Name

Signature